## REMARKS

This amendment responds to the Office Action dated February 27, 2006 and conforms to the parent case Serial No. 09/916,397, filed July 27, 2001. The change to the specification corrects a typographic error in the priority claim. A Supplemental Declaration will be filed shortly.

Claim 1 has been amended to correct a typographic error; "respected" is changed to --respective.-- Claim 46 has been amended to conform to claim 1 and refer to "computer events" and "an attack monitor" which generates "attack warnings." See line 2. The body of the claim earlier referred to "attack warnings". See means for filtering system. Claim 67 has been amended to refer to "said attack monitor." No new matter is added to this case.

In the Office Action on pages 2-12, paragraphs 2-11, the patent examiner rejects all claims 1-67 as being non-patentable in view of certain prior art disclosed in the following references:

U.S. Patent No. 5,960,080 to Fahlman
U.S. Patent No. 6,301,668 to Gleichauf
U.S. Patent No. 5,581,682 to Anderson
U.S. Patent No. 389,542 to Flyntz
U.S. Patent No. 5,036,315 to Gurley
U.S. Patent No. 5,532,950 to Moses et al.
U.S. Patent No. 6,714,977 to Fowler
The 1996 book, Applied Cryptography, by Schneier
The Uniform Resource Locator article "FOLD OC"

In the Office Action, the examiner also issued a double patenting rejection based upon Serial Nos. 09/916,397 (now allowed); 10/008,209; 10/155,525; 10/155,192; 10/277,196; and 10/390,807. Applicant requests that the Examiner withdraw this double patenting rejection since the Examiner did not combine or link the claims in one or more of Serial Nos. 09/916,397 (now allowed); 10/008,209; 10/155,525; 10/155,192; 10/277,196; and 10/390,807 with other prior art.

> ... for a double patenting rejection, the first question to be asked is — does any claim in the application define an invention that is merely an obvious variation of an invention claimed in the patent? If the answer is yes, then an "obviousness-type" nonstatutory double patenting rejection may be appropriate. Obviousness-type double patenting requires rejection of an application claim when the claimed subject matter is **not patentably distinct** from the subject matter claimed in a commonly owned patent, or a non-commonly owned patent but subject to a joint research agreement as set forth in 35 U.S.C. 103(c)(2) and (3), when the issuance of a second patent would provide unjustified extension of the term of the right to exclude granted by a patent. See *Eli Lilly & Co. v. Barr Labs., Inc.*, 251 F.3d 955, 58 USPQ2d 1869 (Fed. Cir. 2001); *Ex parte Davis*, 56 USPQ2d 1434, 1435-36 (Bd. Pat. App. & Inter. 2000). A double patenting rejection of the obviousness-type is "analogous to [a failure to meet] the nonobviousness requirement of 35 U.S.C. 103" except that the patent principally underlying the double patenting rejection is not considered prior art. *In re Braithwaite*, 379 F.2d 594, 154 USPQ 29 (CCPA 1967). Therefore, any analysis employed in an obviousness-type double patenting rejection parallels the guidelines for analysis of a 35 U.S.C. 103 obviousness determination. *In re Braat*, 937 F.2d 589, 19 USPQ2d 1289 (Fed. Cir. 1991); *In re Longi*, 759 F.2d 887, 225 USPQ 645 (Fed. Cir. 1985). Since the analysis employed in an obviousness-type double patenting determination parallels the guidelines for a 35 U.S.C. 103(a) rejection, the factual inquiries set forth in *Graham v. John Deere Co.,* 383 U.S. 1, 148 USPQ 459 (1966), that are applied for establishing a background for determining obviousness under 35 U.S.C. 103 are employed when making an obvious-type double patenting analysis. These factual inquiries are summarized as follows: (A) Determine the scope and content of a patent claim relative to a claim in the application at issue; (B) Determine the differences between the scope and content of the patent claim as determined in (A) and the claim in the application at issue; (C) Determine the level of ordinary skill in the pertinent art; and (D) Evaluate any objective indicia of nonobviousness.
>
> The conclusion of obviousness-type double patenting is made in light of these factual determinations. Any obviousness-type double patenting rejection should make clear: (A) The differences between the inventions defined by the conflicting claims — a claim in the patent compared to a claim in the application; and (B) The reasons why a person of ordinary skill in the art would conclude that the invention defined in the claim at issue would have been< an obvious variation of the invention defined in a claim in the patent.

MPEP § 804(II)(B)(1) p. 800-21

In addition to the failure to link or correlate the claims of the parent case or the other pending applications with prior art, the present system is different than the parent case. No reference refers to "filtering data ... and extracting data ... [wherein] the degree of extraction [is] dependent upon respective ones of said plurality of attack warning." This claim language represents three concepts: (A) degrees of extraction; (B) linked to different attack warnings; and (C) extraction "based upon [said] respective " attack warnings. Without a reference showing (a) multiple types of warnings and (b) specific responses to such multiple warnings and (c) coupled to "degrees of extraction" of data, the presently claimed invention is patentable and is not properly the subject of a double patenting rejection.

It is respectfully submitted that the Examiner withdraw the double patenting rejection.

The presently claimed invention is also patentable because it is drawn to a "multi-level security" system and process and such system and process is patentable and distinct over the cited references. In this case, independent claims 1, 23, 46 refer to "respective extract stores for said plurality of security levels" in the preamble of the claims and to "storing said extracted data and said remainder data in said respective extract stores ... based upon respective ones of said plurality of warnings." See claim 1. It is respectfully submitted that claims 1, 23, 46 all include the concept that various levels of secret data are stored in "respective extract stores" and this is essentially the same as multiple levels of security with multiple levels of secure storage.

In summary, Kirshenbaum '298, Lamm '907 and/or Fahlman '080 do not show, teach or suggest multiple extractions of security sensitive words related to each of a plurality of security levels, and separate storage of those security sensitive words in different secured locations for each security level (multiple extract stores), and the requirement that the user input a password ("security clearance") for each security level. Details of this analysis are set forth in the previously filed amendment. None of these references discuss computer attacks, nor different levels of extraction for different attacks.

Further in summary, Fahlman '080, Andersen '682 and Flyntz '542 do not show, teach or suggest multiple extractions of security sensitive words into a respective plurality of memory stores for each security level (extract stores). Falman '080 does not disclose nor discuss multiple security level storage and retrieval. Anderson '682 describes storing all secure data in a single document (not multiple security storage locations, one for each security level) and Flyntz '542 does not discuss STORING and RETRIEVING different security words from different extract or security memory locations. None of these references discuss computer attacks, nor different levels of extraction for different attacks.

**Kirshenbaum '298** does not show separate storage of secured data, separate and apart from unsecured data. Both secured and non-secured data is stored in a single database 14. Col. 3, lines 40-44; col. 5, lines 7-10 ("The data set is stored in a database ... the document comprises secure portion and non-secure portions"); col. 5, lines 36-37 ("to retrieve those secure and non-secure portions of the document and to send the retrieved portions of the document to the output device.").

**Fahlman '080** does not show, teach or suggest a remainder store for non-secured data, multiple security levels, multiple extraction of security data, storage of multiple levels, presentment of different security codes at each security level. In fact, nowhere does Fahlman '080 discuss password or security clearance control.

**Lamm '907** stores and has multiple copies of all secret-secured data about the consumer in three (3) different computers, to wit, consumer computer 12 (see legends FIG. 2, consumer computer 20, col. 5, line 48), billing - processor computer 26 (see col. 13, line 5) and enrollment server 21 (see col. 9, line 42). The three computers in Lamm '907 provide an integrated bill payment system which cannot be deconstructed into operable components. In contrast, the present invention extracts secured data, for multiple security levels, and then stores the extracted data in extract stores. Lamm's process of storing secret data in three computers is completely different than the claimed system of storing secret data in multiple, extract stores for respective security levels.

**Kluttz '161** does not show, teach or suggest multi-level extract stores nor permitting reconstruction of said data via said extract data stores only in the presence of predetermined security clearances. Kluttz '161 shows utilizing multiple encryption portions in a singular document. See Abstract and FIG. 3. The keys are maintained in the document 100. Col. 6, lines 28-30. FIGS. 5 and 6 show the flowcharts for document decryption which includes utilizing the encryption key in the document itself (step 304, FIG. 5; step 404, FIG. 6). There is no suggestion of utilizing an extracted store and a remainder store.

With respect to **Schneier's book (Applied Cryptography)**, Schneier does not show, teach or suggest multi-level extract stores nor predetermined security clearances, nor reconstruction of said data via multiple extract stores only in the presence of said predetermined security clearances. Schneier discusses encryption and key destruction.

U.S. Patent No. 5,036,315 to **Gurley** does not cure the defects identified above with respect to Lamm '907 and the differences with respect to the present invention. Gurley does not show, teach or suggest (a) filtering data; (b) utilizing multiple extract stores and a remainder store; (c) multiple security clearances for the extract stores; and (d) permitting reconstruction of said data via the multiple extract stores only in the presence of predetermined security clearances. Gurley '315 discusses a video display control which accepts and processes two (2) video signals, one displayed in a defined window of the second video display.

**Flyntz' 572** does not show, teach, or suggest the claimed (i) "filtering data input ... dependent upon ... attack warnings;" (ii) "storing said extracted data ... in respective extract stores;" and (iii) permitting reconstruction of "some or all of said data via said extracted data from ... extract stores ... only in the presence of a predetermined security clearance of said plurality of security clearances." Claim 1. See also, claim 23, 46.

Flyntz '542 is principally interested in retrieving data but the retrieval of data always occurs with a double key system, the first key required is the user's smart card; and the second key required is a mechanical cam switch associated with a removable hard drive containing all complete versions of the secured documents for that security level. Only one memory store at a time is subject to access in Flyntz '542. If the security level on the user's smart card does not match the security level of the removable hard drive, the user is only permitted to retrieve and view unclassified data. Therefore, if the user's smart card has a high level of security rating (secret "S"), and the operable hard drive is designated Classified "C", the user is not permitted access to the C data on the hard drive even though the user's security level is a higher S rating compared with the security code on the hard drive C. Further, in every implementation of the Flyntz '542 patent, if this one to one correspondence (smart card security level must be equal hard drive security level) is NO, the user is only permitted access to the unclassified (U/C) data.

In every instance, Flyntz '542 requires that the smart card used by the user must match the security code of the hard drive (U/C; S; CL) and if not, the user is only permitted to see unclassified data U/C 24. An important feature of the Flyntz '542 system is that the data is on a removable hard drive. Col. 2, line 26 (herein "2/26"); 3/5; 3/31, 5/66; 7/30; 7/35; 7/38; 8/55; 9/41; 10/49; 11/33 ("if the nth memory device were detected by the (n-1)th sensor switch); 11/65; 12/4; 12/30; 12/40; 12/61;

13/15; 13/18; 13/37; 13/67. As explained in detail throughout Flyntz '542, the insertion of this removable hard drive (S or CL) closes a mechanical switch, such as a cam, and the closure of the S or CL drive cam, when matched to the S or CL security level on a smart card of a user, permits the user to access only the secured data on the inserted hard drive and not other data on any other hard drive. Flyntz '542 discusses the required matching between the security level on the user's smart card with the security level on the inserted hard drive memory (S or CL) at the following locations. Col. 2, line 40; Col. 3, lines 28-32; 3/36; 4/2; 5/66; 6/53; 7/30; 8/54; 8/63; 9/55; 10/1; 10/34; 10/49; 11/46; 11/64; 12/39; 12/59; 11/66. Flyntz '542 does not discuss different attack warnings nor different levels of extraction therefor.

**Anderson '682** does not show, teach or suggest storing extract data in respective extract stores in one or more computers and Anderson '682 also does not show, teach or suggest "permitting reconstruction of some or all of said data via said extracted data from respective extract stores only in the presence of a predetermined security clearance of said plurality of security levels." Claim 1. Anderson '682 does not discuss different attack warnings nor different levels of extraction therefor.

Anderson '682 shows that the security information is stored in a single document. For example, looking at the illustrations in Anderson '682, FIG. 2B shows a document and shows a data stream representing that document (see the bottom of the page, rectangular box with five segments including "begin page"). FIG. 3B shows an insert in the document "we should get a better map" which is not shown in the original document FIG. 2B and the added information "we should get a better map" is identified in the "object overlay" shown at the bottom of FIG. 3B after "begin page." FIG. 4 shows another insert in the original document "this needs a nice color picture." In the text of Anderson '682, the disclosure identifies that the document would include triplets (col. 3, line 65, herein "3/65") and theses triplets are shown in the table at 4/11 and include the length of triplet, the type of conditional overlay (normal, annotation or redaction) and the level of the overlay. "The level triplet is compared to one contained within the application being invoked and, if it is equal or lower than the application level, the overlay is processed. Otherwise, the overlay is not performed." 4/37. In applying the Anderson '682 system to a security item, the disclosure states:

> Returning to the decision block 4, if the overlay is a redaction, the system pursues to decision block 8. In decision block 8, the system examines the security level of the redaction and compares it to the security level of the user, which is already known to the system, if the redaction security level exceeds that of the user, the system determines that the user does not have ability to view the documents prior to redaction .

5/3.

Further, Anderson '682 specifically states "at this point, the system returns to block one in order to process any additional overlays that may be found in the current page of the document." Therefore, it is clear that the secure information or secure data in Anderson '682 is included in a single document and that secured data is stored with the document on the computer system. Therefore, Anderson '682 does not show, teach or suggest storing said extracted data in "said respective extract stores" which is a required step in claim 1, and also does not show, teach or suggest "permitting reconstruction of some or all of said data via said extracted data from respective extract stores only in the presence of a predetermined security clearance of said plurality of security levels." Claim 1.

The **FOLDOC** (URL webpage) reference does not discuss multi-level security system claimed herein.

**Moses '950** relates to a dynamic digital filter using a neural network to adjust a digital filter for decoding an audio input signal and for reconstructing a digitized audio signal. The neural network determines whether periodic or aperiodic signals are present and then adjusts the coefficients of the filter. Multi-level security systems are not discussed in Moses '950.

**Wylie**'s book on Survival Information describes a decentralized storage system that "divide[s] the information into multiple pieces, or shares, that can be stored at different storage nodes." p. 62, left col. However, the Wylie system includes a data redundancy feature. p. 62, right col. "As the 'General Threshold Schemes' sidebar describes, a p-m-n threshold scheme breaks information into n shares so that any m of the shares can reconstruct the information and fewer than p shares reveal no information" p. 63, right col. In direct contrast to the presently claimed invention, the Wylie system would not work in that Wylie would store multiple versions or copies of the secret information over multiple storage sites to achieve the p-m-n data redundancy feature. Wylie always employs the p-m-n redundancy feature in his distributed storage system. Storing multiple copies of the same secret data is completely different than the claimed storing a extracted data in respective secret storage stores per the present invention. For example, which security code would one use with the multiple M copies of secured data in the Wylie system? Therefore, the Wylie system is closer to the system in Lamm '907 wherein multiple copies of the same secret information are stored throughout the system and the user can access the same secret information at multiple sites. In the present invention, the secret information is stored one level at a time in multiple, secure extract stores which stores are complimentary to the security level. Wylie teaches away from the present invention as does Lamm '907 since multiple copies of the same secret data are stored at multiple locations.

**Gleichauf '668** discloses an adaptive network security system and FIG. 4 therein shows the use of a system which determines, in step 112, the type of attack (see col. 8, line 28, especially line

36) and then applies the associated response. Priority is assigned based upon the type of attack. "System services are prioritized based upon a level of criticality of each services as can be determined from the network information." Col. 8, line 49. Extracting data wherein "the degree of extraction [is] dependent upon respective ones of said plurality of attack warnings" (claim 1) is not shown nor suggested. Without a reference showing multiple extractions to multiple security levels and attack levels linked to different degrees of extraction, the prior art does not show, teach nor suggest the claimed invention.

**Fowler '977** discloses a monitoring system for a physical space about a computer system and a monitoring system detecting power failure, improper temperature or humidity conditions, or loss of Internet communications. 7/7-25; 8/13-35. Physical conditions, such as temperature and smoke, are monitored. If the sensed condition exceeds a user-set threshold, then an email message is sent to an off-site administrator. 8/50-57. Realtime reports may also be sent. 8/59. The monitor system can be configured to turn ON the AC unit. 15/2. An email message is a typical alarm. 17/16. An SMTP or text message may be sent. 18/7.

Fowler '977 does not operate for multiple attack warnings nor store data "in said respective extract stores ... based upon respective ones of said plurality of attack warnings." Claim 1. Simply because Fowler '977 senses an abnormal condition, it does not show, teach or suggest what to do in multiple "attacks" nor does it show, teach or suggest that data storage occur at multiple levels.

With respect to the **Official Notice**, it is respectfully submitted that the Examiner must identify the source of such knowledge, that a system exists which "increases extraction" upon detection of increasingly higher attack levels. Fowler '977 discusses either an email or web or text message notification or a turn ON signal for an AC unit. These are single event processors, not multiple event processors claimed in the present invention nor does Fowler '977 discuss increasing the output alarm based upon higher attack levels.

The Manual of Patent Examining Procedures ("MPEP") explains that **it is not obvious** to modify a system with a plurality of sensors controlling a plurality of valves to create the inventive and patentable single sensor which controls a plurality of valves:

> In *In re Kotzab,* 217 F.3d 1365, 55 USPQ2d 1313 (Fed.Cir. 2000), the claims were drawn to an injection molding method using a single temperature sensor to control a plurality of flow control valves. The primary reference disclosed a multizone device having multiple sensors, each of which controlled an associated flow control valve, and also taught that one system may be used to control a number of valves. The court found that there was insufficient evidence to show that one system was the same as one sensor. While the control of multiple valves by a single sensor rather than by multiple sensors was a "technologically simple concept," there was no finding "as to the specific, understanding or principle within the knowledge of the skilled artisan" that would have provided the motivation to use a single sensor as the system to control more than one valve. 217 F.3d at 1371, 55 USPQ2d at 1318.

MPEP § 2143.01.

In the present invention, Applicant has developed a system designed to safeguard a plurality of security levels with specific dispersal and retrieval techniques with "the degree of extraction dependent upon respective ones of said plurality of attack warnings." The single data storage systems of the prior art Fahlman '080, Andersen '682, Kluttz '161 and Flyntz '542 or the single reactive alarm systems of Gleichauf '668 and Fowler '977 cannot be extended to the claimed multi-level security storage systems with "the degree of extraction dependent upon respective ones of said plurality of attack warnings." Each of these references discloses single storage of security words based upon a single event.

Applicant respectfully requests that the examiner approve the patentability of claims 1 - 67.

Respectfully submitted,

By ______________________________
Robert C. Kain, Jr.
Reg. No. 30,648
Fleit, Kain, Gibbons, Gutman, Bongini & Bianco, P.L.
750 Southeast Third Avenue, Suite 100
Fort Lauderdale, FL 33316-1153
Telephone: 954-768-9002
Facsimile: 954-768-0158

**Certificate of Mailing**

I hereby certify that this correspondence is being deposited with the U.S. Postal Service as First Class Mail in an envelope addressed to Commissioner for Patents, Mail Stop AF, P.O. Box 1450, Alexandria, VA 22313-1450 on May 25, 2006.

______________________________
Robert C. Kain, Jr.
Reg. No. 30,648

\\Tiger\data share\RCK\CLIENTS\Redlich\Patents\6851-02cip2-amdt-2d-052406.wpd